Organisational Information Security Management Maturity Model

Mazlina Zammani[1]
National Cyber Security Agency
National Security Council
Jalan Impact, 63000, Cyberjaya, Malaysia

Rozilawati Razali[2], Dalbir Singh[3]
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia
43600, Bangi, Selangor, Malaysia

***Abstract*—Information Security Management (ISM) is a systematic initiative in managing the organisation's information security. ISM can also be defined as a strategic approach to addressing information security (IS) risks, breaches, and incidents that could threaten the confidentiality, integrity, and availability of information. Although organisations have complied with ISM requirements, security incidents are still afflicting numerous organisations. This issue shows that the current implementation of ISM is still ineffective. The ineffective ISM implementation illustrates the low maturity level. To achieve a higher level of maturity, organisations should always evaluate their ISM practices. Several maturity models have been developed by international organisations, consultants, and researchers to assist organisations in assessing their ISM practices. However, the current models do not evaluate ISM practices holistically. The measurement dimensions in current models are more focused on assessing certain factors only. This caused the maturity assessment to be not executed comprehensively. Therefore, this study aims to address this shortcoming by proposing a comprehensive maturity assessment model that takes into account ISM success factors to evaluate the effectiveness of the implementation. This study adopted a mixed-method approach, which comprises qualitative and quantitative studies to strengthen the research finding. The qualitative study analyses the existing literature and conducts interviews with nine industry practitioners and six experts while the quantitative study involves a questionnaire survey. The data obtained from the qualitative study were analysed using content analysis while the quantitative data employed statistics analysis. The study identified fourteen success factors and fifty-seven maturity dimensions, which each contains five maturity levels. The proposed model was evaluated through experts' reviews to ensure its accuracy and suitability. The evaluation shows that the model can identify the ISM maturity level systematically and comprehensively. This model will ultimately help the organisations to improve the weaknesses in the implementations thus diminishing security incidents.**

Keywords—*Information security*; *information security management; maturity models; information security management maturity model*

I. Introduction

Now-a-days, organisations' reliance on Information and Communication Technology (ICT) has increased severely due to the rapid development of technology [1],[2],[3],[4],[5]. ICT plays an imperative role in organisations daily operations to ensure the smoothness of the services [6],[7]. In line with the increasing use of ICT in daily operations, organisational information is extremely exposed to security threats and risks [8], [9], [10].

Various efforts have been done to ensure the information is protected. One of the efforts is establishing Information Security Management (ISM). ISM is a strategic approach to addressing information security risks and incidents that could threaten the confidentiality, integrity, and availability of information [10],[11],[12],[13]. However, security incidents endure occurring in organisations [14],[15]. For example, in October 2020, hackers targeted government agencies and telecommunications operators in Iraq, Kuwait, Turkey, and the UAE as part of a cyber espionage campaign [16]. In the latest statistical report released by the National Cyber Coordination and Command Centre, National Cyber Security Agency (NACSA) stated that a total of 4,194 security incidents against public and private organisations were reported in 2020 [17]. This issue shows that the current implementation of ISM is still ineffective [14]. The ineffective ISM implementation illustrates the low maturity level.

Although organisations have complied with ISM requirements set by the industry standards, there is a lack of objective mechanisms to gauge the maturity of the implementation [18]. Even though there are attempts on ISM maturity models [19],[20],[21],[22], they mainly appear as abstract concepts. The current maturity models are typically process-oriented, focusing on measuring security activities and technology aspects without giving much attention to the people aspect, which also contributes to the effectiveness of the ISM implementation [23]. This caused the maturity assessment not executed comprehensively. Thus, the maturity of ISM implementation remains low.

A comprehensive maturity model should consider all aspects in ISM and should not limit to certain aspects only. This study aims to fulfil these needs by proposing a holistic maturity model that considers ISM success factors from four major aspects; People, Process, Organisational Document, and Technology to measure the implementation's effectiveness.

This paper is organised as follows. Section II discussed a review of ISM success factors and the current maturity models. Section III provides the methodology used in this study. Section IV presents the findings and lastly, Section IV summarises the findings.

II. Background

A. ISM Success Factors

ISM provides a strategic direction for implementing security processes and activities to assure security objectives are met, consistent risk management, and effective use of information resources [11],[24]. ISM is likewise a multi-disciplinary discipline that should be given due attention to ensuring an appropriate and secure environment in protecting organisational information [25]. Previous studies have indicated that the success of ISM implementation depends on technical and non-technical factors. Those factors are organised into four aspects: People, Organisational Document, Process, and Technology as listed in Table I.

The people aspect consists of individuals or parties directly involved in the ISM. The organisational document refers to strategic and operational documents that need to be developed and adhered to during ISM implementation. Meanwhile, the process aspects consist of ISM key activities and finally, the technology aspect comprises the use of ICT Infrastructure to support the ISM operations. A comprehensive explanation of the factors and their elements can be found in [26].

B. ISM Maturity

ISM maturity guarantees the successful management of information security [27]. A maturity model is a staged structure where particular security aspects are measured, with the postulation that organisations develop and enhance their ISM implementation from the lowest level to the highest level [27],[28]. Thus far, industries and researchers have developed a few maturity models to assist the organisation in measuring the level of ISM implementation [12],[29].

Control Objectives for Information and Related Technology version 4.1 (COBIT 4.1) is widely used for IT governance [21]. It was developed by IT Governance Institute (ITGI) in the year 2007. This model helps measure an organisation's Information Technology (IT) processes, define a designated maturity level, and improve the process to achieve the preferred maturity level [30]. COBIT 4.1 has six maturity levels, which are from maturity level 0 to maturity level 5.

Another maturity model is Cybersecurity Capability Maturity Model (CMM), developed by Global Cyber Security Capacity Centre in 2014. This model was later revised and improved in 2016 and with a new name Cybersecurity Capability Maturity Model for Nations (CMM). The model allows the organisation to self-assess its current cybersecurity capacity [31]. Conversely, the Open Information Security Management Maturity Model (O-ISM3) by The Open Group assesses maturity based on management processes in four components; general, strategic, tactical, and operational [32]. O-ISM3 has five maturity levels, which look for evidence of the processes in those four components.

Many researchers have adopted the above models in their research work. For example, a study presents a cyclical maturity evaluation model [56] where the maturity level is adopted from COBIT 4.1. The model is based on ISO/IEC 27002 security controls where each implementation of the controls will be assessed. The model outlines eight steps to be followed throughout the assessment. A different researcher proposes a model for measuring ISM performance [46]. The proposed model evaluates the performance based on critical factors, namely, human, processes, risk assessment, and technology. The model contains three maturity levels; basic, intermediate, and advance.

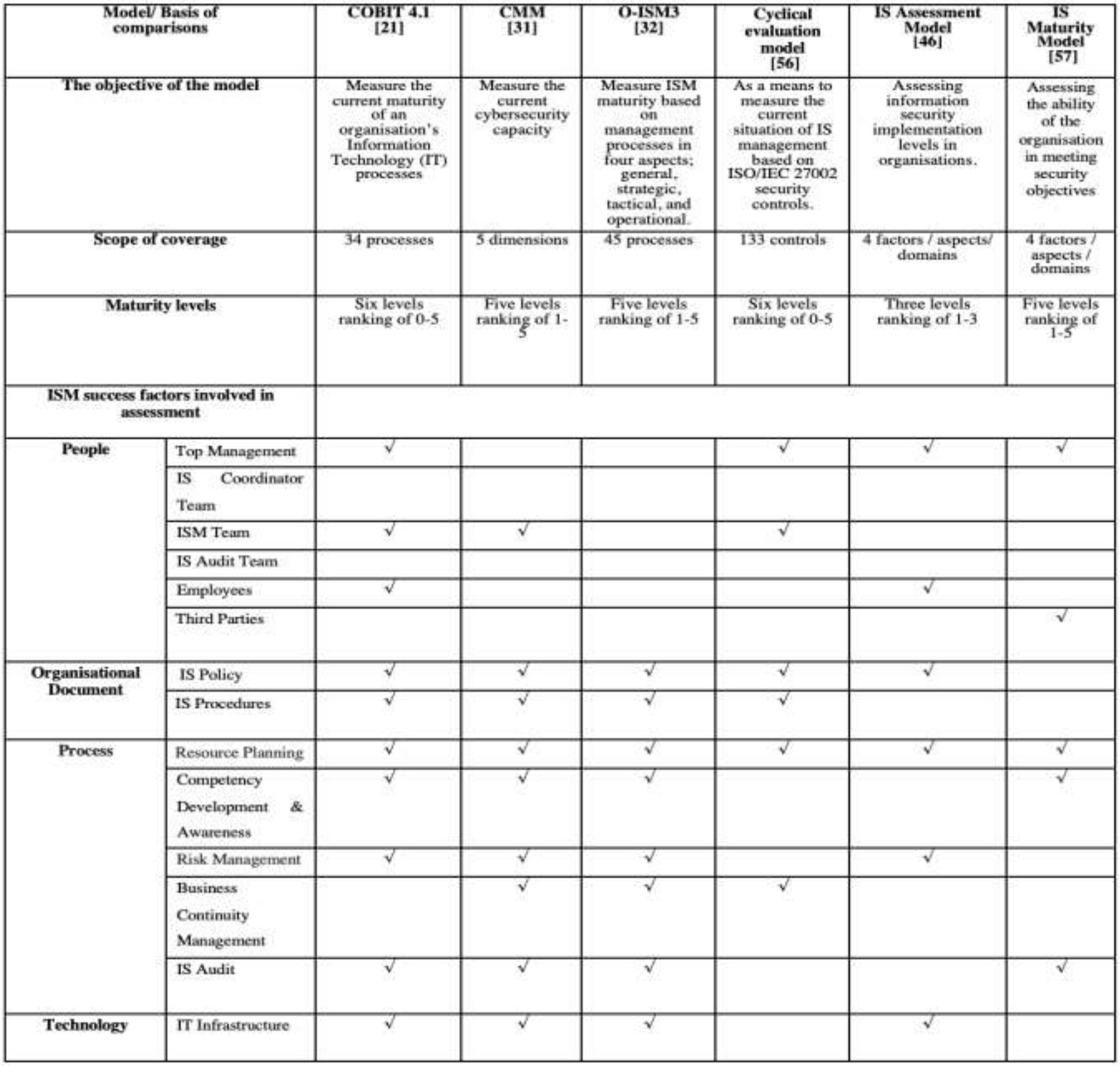
TABLE I. ISM Success Factors

Aspects	*ISM Success Factors*	*Sources*
People	Top Management • knowledge • leadership • commitment	[11],[25],[26],[33],[34],[35] [36],[37],[38],[39],[40],[41] [42],[43],[44]
	IS Coordinator Team • knowledge • commitment • communication skill	[15],[26]
	ISM Team • knowledge • commitment • technical skills • willingness • cooperation	[26],[33],[36],[40],[42],[43],[45]
	IS Audit Team • knowledge • auditing skills • commitment • cooperation • communication skills	[26],[37],[38],[42],[43]
	Employees • awareness • compliance • motivation	[5],[26],[35],[36],[37],[38] [39],[45]
	Third Parties • awareness • compliance	[26],[38],[42],[43],[46]
Organisational Document	IS Policy • clear • comprehensive • communicated • reviewed	[5],[25],[26],[33],[34],[35], [36],[37],[38],[39],[41],[42], [43],[45],[47],[48]
	IS Procedures • clear • complete • communicated • reviewed	[26],[36],[37],[49]
Process	Resource Planning • financial resources • human resource	[26],[33],[34],[35],[38],[42],[43],[45],[50]
	Competency Development Awareness • awareness programs • training programs	[26],[33],[34],[35],[37],[38],[39],[42],[43],[45],[48]
	Risk Management • risk assessment • risk treatment	[25],[26],[35],[36],[37],[38], [41],[42],[43],[45],[48],[51]
	Business Continuity Management • plan • simulation	[26],[37],[38],[41],[49],[52]
	IS Audit • audit program • audit finding & reporting • follow-up audit	[26],[36],[37],[38],[42],[43], [53]
Technology	IT Infrastructure • software • hardware	[5],[26],[36],[38],[42],[43], [45],[50],[54],[55]

On the other hand, a maturity model developed by [57] aims to assess the organisation's ability to meet security objectives. The model defines the process of managing, measuring, and controlling security based on four aspects; governance, security management, system architecture, and service management. Each aspect has its indicators [12]. This model has five levels of compliance which starting from non-compliance to full compliance.

The comparison of the mentioned models is summarised in Table II. Table II shows several ISM success factors are being considered as the maturity dimensions in the existing model. However, the existing models are typically process-oriented which focus more on the process and technology factors and have less emphasis on the people factors. This causes the implementation of ISM is evaluated less comprehensively. People factors play a significant role in ISM [58]; thus, need to be emphasized as well [59]. Therefore, a holistic maturity model is required by incorporating all ISM success factors and their elements to ensure the effectiveness of the ISM implementation.

TABLE II. COMPARISON OF MATURITY MODELS



Model/ Basis of comparisons		COBIT 4.1 [21]	CMM [31]	O-ISM3 [32]	Cyclical evaluation model [56]	IS Assessment Model [46]	IS Maturity Model [57]
The objective of the model		Measure the current maturity of an organisation's Information Technology (IT) processes	Measure the current cybersecurity capacity	Measure ISM maturity based on management processes in four aspects; general, strategic, tactical, and operational.	As a means to measure the current situation of IS management based on ISO/IEC 27002 security controls.	Assessing information security implementation levels in organisations.	Assessing the ability of the organisation in meeting security objectives
Scope of coverage		34 processes	5 dimensions	45 processes	133 controls	4 factors / aspects/ domains	4 factors / aspects / domains
Maturity levels		Six levels ranking of 0-5	Five levels ranking of 1-5	Five levels ranking of 1-5	Six levels ranking of 0-5	Three levels ranking of 1-3	Five levels ranking of 1-5
ISM success factors involved in assessment							
People	Top Management	√			√	√	√
	IS Coordinator Team						
	ISM Team	√	√		√		
	IS Audit Team						
	Employees	√				√	
	Third Parties						√
Organisational Document	IS Policy	√	√	√	√	√	
	IS Procedures	√	√	√	√		
Process	Resource Planning	√	√	√	√	√	√
	Competency Development & Awareness	√	√	√			√
	Risk Management	√	√	√		√	
	Business Continuity Management		√	√	√		
	IS Audit	√	√	√			√
Technology	IT Infrastructure	√	√	√		√	

III. Methodology

This study adopts the mixed-method approach, which comprises both qualitative and quantitative data collection and analysis. This approach involves four main phases: theoretical, empirical, model development, and model validation. Fig. 1 illustrates the research design.

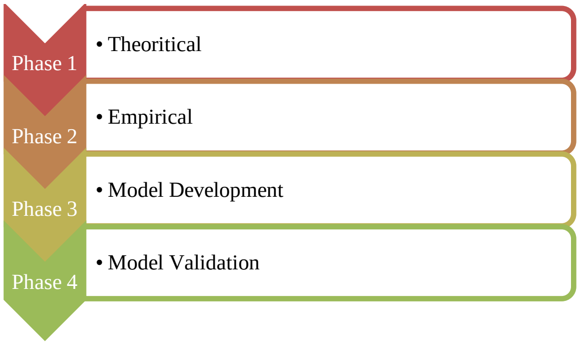


Fig. 1. Research Design.

A. Phase 1: Theoretical

The theoretical study reviewed published and unpublished documents in multiple online databases such as ACM Digital Library, Web of Science, Science Direct, Google Scholar, Pro-quest, IEEE Explorer, Mendeley and CiteSeer to identify the ISM success factors and ISM maturity models. The selected documents were then analysed qualitatively using content analysis. The preliminary findings of this study have been reported in [44].

B. Phase2: Empirical

The empirical study is to verify the success factors and identify each success factor's maturity dimension and levels. As it involves various aspects, it is thus divided into three parts:

- Empirical I: The purpose of Empirical I is to verify the ISM success factors derived from the theoretical study and discover other relevant factors from practitioners' views. This study used semi-structured interviews. A series of individual and focus group interviews with experienced ISM practitioners was conducted. The findings of this study have been reported in [26].
- Empirical II: The purpose of Empirical II is to confirm and refine the findings of Empirical I through a large-scale survey. A total of 400 questionnaires were sent to respondents in public and private agencies. The data collected from the survey were analysed using Statistical Analysis. The findings of this empirical II have been reported in [60].
- Empirical III: A series of interviews with six experts were conducted to identify the ISM maturity dimensions and levels. The selection of experts was based on their experience, knowledge, and expertise in ISM. Contents analysis technique was used to analyse the data.

C. Phase 3: Model Development

The ISM maturity model was developed using the findings from Empirical I, II, and III. The identified success factors, dimensions, and levels were used as the components in the maturity model.

The development of this maturity model is guided by the International Standards ISO / IEC 33004: 2015 Information technology - Process assessment - Requirements for process reference, process assessment and maturity models [61]. In addition, the measurement theory of [62] and [63], which introduced the ordinal scale, was also used as a basis in the development of this ISM maturity model.

D. Phase 4: Model Validation

This phase evaluates the accuracy of the proposed model through expert review. A series of interviews with three experts were conducted to evaluate the accuracy and suitability of the proposed model. Based on the review, the proposed model was improved.

IV. Result and Finding

Based on the experts reviewed, the final Organisational ISM Maturity Model has 4 aspects, 14 factors, 42 elements, and 57 maturity dimensions. The 14 factors are grouped under four main aspects namely People, Organisational Document, Process and Technology. Each factor has its own elements. Each element has specific dimensions. Each dimension has five levels of maturity; maturity level 1 to maturity level 5 where Level 1 is the lowest level of maturity while Level 5 is the highest level of maturity. The finalised Organisational ISM maturity model is shown in Table III.

This study has produced a comprehensive model of measuring organisational ISM maturity. In contrast to the existing model, this Organisational ISM Maturity Model contains factors from process and technology aspects and contains factors from non-technical aspects, namely People and Organisational Document. Every identified factor was then sorted according to its categories and subsequently determined its maturity dimensions. Based on the arrangement of categories and factors generated, this study helps the organisations to self-assessing the maturity level of their ISM implementation systematically. Through the assessment conducted, the organisation can identify their ISM maturity level while further improving the implementation of their ISM.

TABLE III. ORGANISATIONAL INFORMATION SECURITY MANAGEMENT MATURITY MODEL

Aspects	Factors	Elements	Maturity Dimensions	Level 1	Level 2	Level 3	Level 4	Level 5
People	Top Management	Leadership	Personnel/unit involvement in ISM	ISM implementation involves only the ICT unit.	ISM implementation involves ICT unit and process owners.	ISM implementation involves the ICT unit, process owners, and administrative unit.	ISM implementation involves the ICT unit, process owner, administrative unit, and responsible units.	ISM implementation involves the ICT unit, process owners, administrative unit, responsible units, and stakeholders.
		Knowledge	The percentage of understanding the objectives and security issues.	Less than 25% of objectives and security issues are understood.	At least 25% of the objectives and security issues are understood.	At least 50% of the objectives and security issues are understood.	At least 75% of the objectives and security issues are understood.	100% security objectives and issues are understood.
		Commitment	The response rate on the ISM issue.	The response to the ISM issues is very slow.	The response to the ISM issues is slow.	The response to the ISM issues is fairly fast.	The response to the ISM issues is fast.	The response to the ISM issues is very fast.
	IS Coordinator Team.	Knowledge	The percentage of IS Coordinator Team members understand the needs, governance, and processes of ISM.	Less than 25% of IS Coordinator Team members understand the needs, governance, and processes of ISM.	At least 25% of the IS Coordinator Team members understand the needs, governance, and processes of ISM.	At least 50% of the IS Coordinator Team members understand the needs, governance, and processes of ISM.	At least 75% of the IS Coordinator Team members understand the needs, governance, and processes of ISM.	100% of the IS Coordinator Team members understand the needs, governance, and processes of ISM.
		Commitment	The percentage of the ISM planning schedule is achieved.	Less than 25% of the ISM planning schedule is achieved.	At least 25% of the ISM planning schedule is achieved	At least 50% of the ISM planning schedule is achieved.	At least 75% of the ISM planning schedule is achieved.	100% of the ISM planning schedule is achieved.
		Communication Skills	The clarity of the information presented.	Very unclear.	Unclear.	Quite clear.	Clear.	Very clear.
			The attitude of IS Coordinator Team members when communicating	Being not open and not persuasive.	Being less open and less persuasive.	Being a little open and a little persuasive.	Being open and persuasive.	Being very open and very persuasive.
	ISM Team	Knowledge	The percentage of ISM team members are knowledgeable in IS domain.	Less than 25% of ISM team members are knowledgeable in IS domain.	At least 25% of ISM team members are knowledgeable in IS domain.	At least 50% of ISM team members are knowledgeable in IS domain.	At least 75% of ISM team members are knowledgeable in IS domain.	100% of ISM team members are knowledgeable in IS domain.
		Technical Skills	The average duration of ISM team members' involvement in implementing IS operations.	Less than 1 year.	Between 1 - 2 years.	Between 2 - 3 years.	Between 3 - 4 years.	Over 4 years.
			The capability of ISM team members to complete IS operations.	Unable to complete IS operations at a specific time without support from consultants.	Slightly capable to complete IS operations at specific times without support from consultants.	Moderately capable to complete IS operations at specific times without support from consultants.	Capable to complete IS operations at specific times without support from consultants.	Very capable to complete IS operations at specific times without support from consultants.
		Commitment	The percentage of ISM team members committed to implementing IS operations.	Less than 25% of ISM team members committed to implementing IS operations.	At least 25% of ISM team members committed to implementing IS operations.	At least 50% of ISM team members committed to implementing IS operations.	At least 75% of ISM team members committed to implementing IS operations.	100% of ISM team members committed to implementing IS operations.

			The percentage of ISM team members follow security procedures.	Less than 25% of ISM team members follow the security procedures.	At least 25% of ISM team members follow the security procedures.	At least 50% of ISM team members follow the security procedures.	At least 75% of ISM team members follow the security procedures.	100% of ISM team members follow the security procedures.
		Willingness	The percentage of ISM team members willing to accept and implement changes.	Less than 25% of ISM team members willing to accept and implement changes.	At least 25% of ISM team members willing to accept and implement changes.	At least 50% of ISM team members willing to accept and implement changes.	At least 75% of ISM team members willing to accept and implement changes.	100% of ISM team members willing to accept and implement changes.
		Cooperation	Level of understanding between ISM team members to achieve IS objectives.	There is no understanding to achieve IS objectives.	Lack of understanding to achieve IS objectives.	Quite understanding to achieve IS objectives.	Understanding to achieve IS objectives.	Very understanding to achieve IS objectives.
	IS Audit Team	Knowledge	The percentage of IS audit team members are knowledgeable in IS standards.	Less than 25% of IS audit team members are knowledgeable in IS standards.	At least 25% of IS audit team members are knowledgeable in IS standards.	At least 50% of IS audit team members are knowledgeable in IS standards.	At least 75% of IS audit team members are knowledgeable in IS standards.	100% of IS audit team members are knowledgeable in IS standards.
			The percentage of IS audit team members are knowledgeable in the ISM scope of the audited organisation.	Less than 25% of IS audit team members are knowledgeable in the ISM scope of the audited organisation.	At least 25% of IS audit team members are knowledgeable in the ISM scope of the audited organisation.	At least 50% of IS audit team members are knowledgeable in the ISM scope of the audited organisation.	At least 75% of IS audit team members are knowledgeable in the ISM scope of the audited organisation.	100% of IS audit team members are knowledgeable in the ISM scope of the audited organisation.
		Auditing skills	The frequency of audit team members' involvement in internal and external audit within 3 years.	1 time involved in internal/external audit.	2 times involved in internal/external audit.	3 times involved in internal/external audit.	4 times involved in internal/external audit.	More than 4 times involved in internal/external audit.
		Commitment	Level of detail in writing audit notes.	Not detailed.	Lack of detail.	Quite Detailed	Detailed.	Very detailed.
		Cooperation	The work culture of IS audit team members during audit findings discussion.	No cooperation during audit findings discussion.	Lack of co-operation during audit findings discussion.	Quite cooperate during audit findings discussion.	Cooperate during audit findings discussion.	Strongly cooperate during audit findings discussion.
		Communication Skills	The clarity of information delivery (oral and written).	Very unclear.	Unclear.	Quite clear.	Clear.	Very clear.
	Employee	Awareness	The percentage of employees' awareness toward IS policy.	Less than 25% of employees are aware of IS policy.	At least 25% of employees are aware of IS policy.	At least 50% of employees are aware of IS policy.	At least 75% of employees are aware of IS policy.	100% of employees aware of IS policy.
		Compliance	The percentage of employees' compliance with IS policy.	Less than 25% of employees comply with IS policy.	At least 25% of employees comply with IS policy.	At least 50% of employees comply with IS policy.	At least 75% of employees comply with IS policy.	100% of employees comply with IS policy.
		Motivation	The frequency of employees receiving appreciation.	Never received an appreciation.	Rarely receive an appreciation.	Quite often receive appreciation.	Often receive appreciation.	Very often receive appreciation.
	Third parties	Awareness	The percentage of third parties' awareness toward IS policy.	Less than 25% of third parties are aware of IS policy.	At least 25% of third parties are aware of IS policy.	At least 50% of third parties are aware of IS policy.	At least 75% of third parties are aware of IS policy.	100% of third parties are aware of IS policy.
		Compliance	The percentage of third parties' compliance with IS policy and contracts.	Less than 25% of third parties comply with IS policy and contracts.	At least 25% of third parties comply with IS policy and contracts.	At least 50% of third parties comply with IS policy contracts.	At least 75% of third parties comply with IS policy contracts.	100% of third parties comply with IS policy and contracts.

0rg. Document	IS Policy	Clear	The percentage of IS policy contents that outlines the objectives, controls, and responsibilities of the parties involved are understood by the reader.	Less than 25% of IS policy contents are understood by readers.	At least 25% of the IS policy contents are understood by the reader.	At least 50% of the IS policy contents are understood by the reader.	At least 75% of the IS policy contents are understood by the reader.	100% of the IS policy contents are understood by the reader.
		Comprehensive	The percentage of security controls established is based on the recommendations of international standards and IS requirements.	Less than 25% of security controls are established based on the recommendations of international standards and IS requirements.	At least 25% of security controls are established based on the recommendations of international standards and IS requirements.	At least 50% of security controls are established based on the recommendations of international standards and IS requirements.	At least 75% of security controls are established based on the recommendations of international standards and IS requirements.	100% security controls are established based on the recommendations of international standards and IS requirements.
		Communicated	The frequency of IS policy dissemination.	Once a year.	2 times a year.	3 times a year.	4 times a year.	More than 4 times a year.
			The number of IS policy dissemination mediums.	1 medium.	2 mediums.	3 mediums.	4 mediums.	More than 4 mediums.
		Reviewed	The percentage of IS policy contents is reviewed/ updated according to current needs.	Less than 25% of IS policy contents are reviewed/ updated according to current needs.	At least 25% of IS policies contents are reviewed /updated according to current needs.	At least 50% of the IS policy contents are reviewed/ updated according to current needs.	At least 75% of IS policy contents are rereviewed/ updated according to current needs.	100% IS policy contents are reviewed/ updated according to current needs.
	IS Procedures	Clear	The percentage of IS procedures understood by the personnel/ team in charge.	Less than 25% of IS procedures are understood by the personnel/ team in charge.	At least 25% of IS procedures are understood by the personnel/ team in charge.	At least 50% of IS procedures are understood by the personnel/ team in charge.	At least 75 % of IS procedures are understood by the personnel/ team in charge.	100% IS procedures are understood by the personnel/ team in charge.
		Complete	The level of IS procedures feasibility.	Most of the procedures are very difficult to implement/ follow.	Most of the procedures are difficult to implement/ follow.	Most of the procedures are quite easy to implement/ follow.	Most of the procedures are easy to implement/ follow.	Most of the procedures are very easy to implement/ follow.
		Communicated	The frequency rate of the IS procedures communicated.	Most of the procedures are not communicated to the responsible officer.	Most of the procedures are rarely communicated to the responsible officer.	Most of the procedures are communicated to the responsible officer regularly.	Most of the procedures are communicated to the responsible officer as required.	Most of the procedures are communicated to the responsible officer periodically and as required.
		Reviewed	The Percentage of IS procedures reviewed/ updated according to current needs.	Less than 25% of IS procedures are reviewed/ updated according to current needs.	At least 25% of IS procedures are reviewed/ updated according to current needs.	At least 50% of IS procedures are reviewed/ updated according to current needs.	At least 75% of IS procedures are rereviewed/ updated according to current needs.	100% content of IS procedures reviewed/ updated according to current needs.
Process	Resource Planning	Financial resources	The amount of financial allocation to support the implementation of the ISM.	Very insufficient.	Insufficient.	Quite sufficient.	Sufficient.	Very sufficient and is given priority in the allocation application every year.
		Human Resources	The number of officers performing security operations.	Very insufficient	Insufficient.	Quite sufficient.	Sufficient.	Very sufficient.
			The competency level of allocated officers.	Not competent.	Lack of competence.	Quite competent.	Competent.	Very competent.

	Competency Development & Awareness	Training Programmes	The suitability of the training programmes given to employees and team members.	Most of the training programs given to staff and team members do not suit the work scope.	Most of the training programs given to staff and team members are less suited to the work scope.	Most of the training programs given to staff and team members are quite suited to the work scope.	Most of the training programs given to staff and team members are suited to the work scope.	Most of the training programs given to staff and team members are well suited to the work scope.
			The knowledge of the employees and team members after attending training programs.	Very low.	Low.	Moderate.	Good.	Excellent.
		Awareness Programmes	The number of awareness programs mediums in a year.	Awareness programs are implemented through 1 medium.	Awareness programs are implemented through 2 mediums.	Awareness programs are implemented through 3 mediums.	Awareness programs are implemented through 4 mediums.	Awareness programs are implemented in more than 4 mediums.
			The frequency of awareness programs in a year.	Once a year.	Twice a year.	3 times a year.	4 times a year.	More than 4 times a year.
			The percentage of security incidents has been reduced.	Less than 25% of security incidents have been reduced.	At least 25% of security incidents have been reduced.	At least 50% of security incidents have been reduced.	At least 75% of security incidents have been reduced.	100% security incidents have been reduced.
	Risk management	Risk Assessment	The percentage of process owners, asset owners and IS team's involvement in risk assessment.	Less than 25%.	At least 25%.	At least 50%.	At least 75%.	100%.
			The percentage of assets (included in the scope) that have been assessed.	Less than 25% of assets have been assessed.	At least 25% of the assets have been assessed.	At least 50% of the assets have been assessed.	At least 75% of the assets have been assessed.	100% of the assets have been assessed.
		Risk Treatment	Level of treatment suitability in managing risk.	Not appropriate	Less appropriate	Quite appropriate.	Appropriate.	Very appropriate.
			Percentage of high-risk assets that have been depreciated.	Less than 25%.	At least 25%.	At least 50%.	At least 75%.	100%.
	Business continuity and incident management	Plan	The percentage of plan availability.	Less than 25%.	At least 25%.	At least 50%.	At least 75%.	100%.
			The percentage of incidents and disasters successfully handled (identified, reported, recovered) within a set time.	Less than 25%.	At least 25%.	At least 50%.	At least 75%.	100%.
		Simulation	Diversity of simulation implementation over 5 years.	The same simulation was implemented over 5 years.	At least 2 different simulations were implemented over 5 years.	At least 3 different simulations were implemented over 5 years.	At least 4 different simulations were implemented over 5 years.	More than 4 different simulations were implemented over 5 years.
	IS Audit	Audit program	The level of audit scope.	The scope of the audit is not comprehensive.	The scope of the audit is less comprehensive.	The scope of the audit is quite comprehensive.	The scope of the audit is comprehensive.	The scope of the audit is comprehensive and has value-added.

		Audit Findings and Reporting	The clarity percentage of the audit findings and reporting.	Less than 25% of audit findings are clearly reported.	At least 25% of audit findings are clearly reported.	At least 50% of audit findings are clearly reported.	At least 75% of audit findings are clearly reported.	100% of audit findings are clearly reported.
		Follow-up Audit	The level of follow-up audit review.	The revision of the corrective and preventive actions is carried out incomplete.	The revision of the corrective and preventive actions is carried out less completely.	The revision of corrective and preventive actions is carried out quite completely.	The revision of the corrective and preventive actions is carried out completely.	The revision of the corrective and preventive actions is carried out completely and thoroughly.
			The accuracy percentage of the implementation of the preventive and corrective actions.	Less than 25% of corrective and preventive actions are implemented appropriately.	At least 25% of corrective and preventive actions are implemented appropriately.	At least 50% of corrective and preventive actions are implemented appropriately.	At least 75% of corrective and preventive actions are implemented appropriately.	100% of corrective and preventive actions are implemented appropriately.
Technology	IT Infrastructure	Hardware	The percentage of hardware maintenance.	Less than 25% of hardware is maintained on schedule.	At least 25% of the hardware is maintained on schedule.	At least 50% of the hardware is maintained on schedule.	At least 75% of the hardware is maintained on schedule.	100% hardware is maintained on schedule.
			The percentage of latest hardware used.	Less than 25% of the latest hardware is used.	At least 25% of the latest hardware is used.	At least 50% of the latest hardware is used.	At least 75% of the latest hardware is used	100% up-to-date hardware is used.
		Software	The percentage of software maintenance (updated version/security features in software architecture).	Less than 25% of software is maintained on schedule.	At least 25% of the software is maintained on schedule.	At least 50% of the software is maintained on schedule.	At least 75% of the software is maintained on schedule.	100% software is maintained on schedule.
			The percentage of use of software security functions.	Less than 25% of software security functions are used.	At least 25% of software security functions are used.	At least 50% of software security functions are used.	At least 75% of software security functions are used.	100% software security functions are used.

V. Conclusion

ISM is a strategic approach to address IS risks and breaches as well as to reduce IS incidents that can compromise the confidentiality, integrity and availability of organisational information. These IS risks, incidents and breaches can be minimised if the organisation implements ISM effectively. The effectiveness of ISM can be achieved if organisations assess the maturity of their ISM practices using a holistic maturity model. A holistic maturity model needs to consider the ISM success factors in every aspect to ensure that the assessment is made comprehensively.

This study has successfully developed a holistic maturity model to help organisations in self-assessing the maturity level of their ISM implementation. This initiative encourages organisations to continue improving the implementation of their ISM from time to time. This model can also be used as guidelines and references to academicians and researchers involved in information security maturity.

Finally, here are some suggestions for further research that can be implemented in the future:

- Specialise the model according to the type of organisation.

This study does not specialise in any particular type of organisation, whether public or private organisation. The nature of service is quite different between those two sectors, and it is believed that organisations in both sectors have relatively slightly different information security controls. Accordingly, detailed studies by the type of organisation can be done in the future to produce a more accurate model.

- Automate the maturity model.

Further studies are proposed to automate the Organisational ISM Maturity Model. The automated ISM maturity model not only simplifies the evaluation process but can also be used for record-keeping and report generating. This allows the organisation to monitor the progress of the ISM, compare the maturity level obtained each year, as well as predict the level of maturity that will be obtained in subsequent years more easily.

Acknowledgment

The authors would like to thank Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia for supporting this research. The authors also thank the practitioners and experts who participated in this study.

References

[1] Mirtsch, M., Blind, K., Koch, C. and Dudek, G., “Information security management in ICT and non-ICT sector companies: A preventive innovation perspective,” Computers & Security 109, pp. 1-23, 2021.

[2] Chu, A.M. and So, M.K., “Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective,” Sustainability vol. 12 no. 8, pp. 3163 – 3187, 2020.

[3] Napitupulu, Darmawan. "A conceptual model of e-government adoption in Indonesia." International Journal on Advanced Science, Engineering and Information Technology 7, vol. 4, pp. 1471-1478, 2017.

[4] Kadhum, Ahmed Meri, and Mohamad Khatim Hasan. "Assessing the determinants of cloud computing services for utilizing health information systems: A case study." International Journal on Advanced Science, Engineering and Information Technology vol.7, no. 2, pp. 503-510, 2017.

[5] S. Woodhouse, “Critical Success factors for an Information Security Management System,” in 5th International Conference on Information Technology and Applications ICITA 2008, 2008, no. Icita, pp. 244–249.

[6] Jere, Joseph N., and Nsikelelo Ngidi, "A technology, organisation and environment framework analysis of information and communication technology adoption by small and medium enterprises in Pietermaritzburg," South African Journal of Information Management, vol. 22 no. 1, pp. 1-9, 2020.

[7] Witarsyah, Deden, et al. "The critical factors affecting E-Government adoption in Indonesia: A conceptual framework." International Journal on Advanced Science, Engineering and Information Technology, vol. 7, no. 1, pp. 160-167, 2017.

[8] Ključnikov, A., Mura, L. and Sklenár, D, “Information security management in SMEs: factors of success,” Entrepreneurship and Sustainability Issues vol. 6 no. 4, pp. 2081-2094, 2019.

[9] Khan, Navid Ali, Sarfraz Nawaz Brohi, and Noor Zaman, "Ten deadly cyber security threats amid COVID-19 pandemic," TechRxiv Powered by IEEE, 2020.

[10] Tu, C.Z., Yuan, Y., Archer, N. and Connelly, C.E., “Strategic value alignment for information security management: A critical success factor analysis,” Information & Computer Security, pp. 1-28. 2018.

[11] Rahayu, H. and Rozilawati, R., “Contributing Factors for Successful Information Security Management Implementation: A Conceptual Model,” International Journal of Innovative Technology and Exploring Engineering (IJITEE) vol. 9, no.2, pp. 4491-4499, 2019.

[12] Makupi, D. and Masese, N., “Determining Information Security Maturity Level of an organization based on ISO 27001,” International Journal of Computer Science and Engineering vol. 6, no. 7, pp. 5-11, 2019.

[13] Singh, A.N. and Gupta, M.P., “Information security management practices: case studies from India,” Global Business Review vol. 20, no. 1, pp. 253-271, 2019.

[14] Rahayu, H. and Razali, R., “Contributing Factors for Successful Information Security Management Implementation: A Preliminary Review." The Interdisciplinary Of Management, Economic And Social Research, pp. 12-22, 2020.

[15] R. Hashim and R. Razali, “Contributing Factors for Successful Information Security Management Implementation: A Preliminary Review,” The Interdisciplinary Of Management, Economic And Social Research, vol. 9, no.2, p.12, 2019.

[16] Center for Strategic and International Studies (CSIS), “Significant Cyber Incidents Since 2006.” 2021.

[17] National Cyber Security Agency. Cyber Security Incident Statistics. 2020.

[18] Schmid, M. and Pape, S., “A structured comparison of the corporate information security maturity level,” IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 223-237, 2019.

[19] M. F. Saleh, “Information Security Maturity Model,” Int. J. Comput. Sci. Secur., vol. 5, no. 3, p. 21, 2011.

[20] T. Dirgahayu and D. Ariyadi, “Assessment to C OBIT 4 . 1 Maturity Model Based on Process Attributes and Control Objectives,” in 2015 International Conference on Science in Information Technology (ICSITech), 2015, pp. 343–347.

[21] ITGI, The Control Cbjectives for Information and Related Technology (COBIT 4.1). 2007.

[22] V. C. Aceituno, “Ism3 1.0. Information Security Management Maturity Model,” 2004.

[23] W. Sung and S. Kang, “An empirical study on the effect of information security activities: focusing on technology, institution, and awareness,” Proceedings of the 18th Annual International Conference on Digital Government Research, pp. 84–93, 2017.

[24] A. S. Lima, J. N. de Souza, E. C. Branco, and M. Ribas, “Towards value-based information security management monitoring,” Integr. Netw. Manag. (IM 2013), 2013 IFIP/IEEE Int. Symp., pp. 1260–1267, 2013.

[25] S. Dzazali and A. H. Zolait, “Assessment of information security maturity: An exploration study of Malaysian public service organizations,” J. Syst. Inf. Technol., vol. 14, no. 1, pp. 23–57, 2012.

[26] M. Zammani and R. Razali, “An Empirical Study of Information Security Management Success Factors,” Int. J. Adv. Sci. Eng. Inf. Technol., vol. 6, no. 6, pp. 904–913, 2016.

[27] O. Matrane, M. Talea, C. Okar, and A. Talea, “Towards A New Maturity Model for Information System,” 2015 Int. J. Comput. Sci. Issues, vol. 3, no. 12, pp. 268–275, 2015.

[28] K. Randeree, A. Mahal, and A. Narwani, “A business continuity management maturity model for the UAE banking sector,” Bus. Process Manag. J., vol. 18, no. 3, pp. 472–492, 2012.

[29] J.V. Carvalho, A. Rocha, R. van de Wetering and A. Abreu, “A Maturity model for hospital information systems,” Journal of Business Research, 94, pp. 388-399, 2019.

[30] C. S. Leem, B. W. Kim, E. J. Yu, and M. H. Paek, “Information technology maturity stages and enterprise benchmarking: an empirical study,” Ind. Manag. Data Syst., vol. 108, no. 3, pp. 1200–1218, 2008.

[31] G. C. S. C. C. GSCSCC, Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition, no. CMM. 2016.

[32] TOG, Open Information Security Management Maturity Model. The Open Group, 2011.

[33] N. Ibrahim and N. Ali, “The Role of Organizational Factors to the Effectiveness of ISMS Implementation in Malaysian Public Sector,” Int. J. Eng. Technol., vol. 7, no. 4.35, pp. 544–550, Nov. 2018.

[34] P. K. Sari, N. Nurshabrina, and Candiwan, “Factor Analysis on Information Security Management in Higher Education Institutions,” in 4th International Conference on Cyber and IT Service Management, pp. 1-5. IEEE, 2016., 2016, pp. 1–5.

[35] M. a. Alnatheer, “Information Security Culture Critical Success Factors,” in 2015 12th International Conference on Information Technology - New Generations, 2015, pp. 731–735.

[36] P. Bowen, J. Hash, and M. Wilson, NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers, no. October. Maryland, USA: National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security, 2006.

[37] A. N. Singh, M. P. Gupta, and A. Ojha, “Identifying factors of ‘organizational information security management,’” J. Enterp. Inf. Manag., vol. 27, no. 5, p. 8, 2014.

[38] M. Chander, S. K. Jain, and R. Shankar, “Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach,” J. Model. Manag., vol. 8, no. 2, pp. 171–189, 2013.

[39] M. Kazemi, H. Khajouei, and H. Nasrabadi, “Evaluation of information security management system success factors: Case study of Municipal organization,” African J. Bus. Manag., vol. 6, no. 14, pp. 4982–4989, 2012.

[40] N. Maarop, N. Mustapha, R. Yusoff, R. Ibrahim, and N. M. M. Zainuddin, “Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation,” Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng., vol. 9, no. 3, pp. 884–889, 2015.

[41] A. Cartlidge et al., An Introductory Overview of ITIL® 2011. Orwich: TSO (The Stationery Office), 2012.

[42] COBIT v 5, COBIT for information security. Rolling Meadows, IL: ISACA, 2012.

[43] ISO, “ISO / IEC 27001: Information Technology – Security Techniques –Information Security Management System – Requirements,” 2013.

[44] M. Zammani and R. Razali, “Information security management success factors,” Adv. Sci. Lett., vol. 22, no. 8, 2016.

[45] MAMPU, CGSO, C. Malaysia, and MIMOS, “Rangka Kerja Keselamatan Siber Sektor Awam,” 2016.

[46] M. A. Mohamad Stambul; and R. Razali, “An assessment model of information security implementation levels,” in Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, 2011, pp. 1–6.

[47] A. Azhari, “Ke Arah Implementasi Sistem Polisi Keselamatan ICT Kajian Kes : Pusat Teknologi Maklumat dan Komunikasi,” Universiti Teknologi Malaysia, 2008.

[48] Q. Hu, T. Dinev, P. Hart, and D. Cooke, “Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture ∗,” Decis. Sci. J., vol. 00, no. 00, pp. 1–45, 2012.

[49] ISO, “ISO / IEC 27002: Information Technology - Security techniques - Code of practice for information security controls,” 2013.

[50] R. Diesch, M. Pfaff, and H. Krcmar, “A comprehensive model of information security factors for decision-maker,” Computers & Security, 92, p. 101747, 2020.

[51] M. S. Saleh and A. Alfantookh, “A new comprehensive framework for enterprise information security risk management,” Appl. Comput. Informatics, vol. 9, no. 2, pp. 107–118, 2011.

[52] N. Aisyah, S. Abdullah, N. L. Noor, E. Nuraihan, and M. Ibrahim, “Contributing Factor To Business Continuity Management (Bcm) Failure – a Case of Malaysia Public Sector,” in Proceedings of the 5th International Conference on Computing and Informatics, ICOCI, 2015, no. 077, pp. 530–538.

[53] S. Islam, N. Farah, and T. F. Stafford, “Factors associated with security / cybersecurity audit by internal audit function An international study function,” Manag. Audit. J., vol. 33, no. 4, pp. 377–409, 2018.

[54] A. A. Norman and N. M. Yasin, “Information Systems Security Management (ISSM) Success Factor: Retrospection From the Scholars,” Proceedings of the 11th European Conference on Information Warfare and Security, no. July 2012. pp. 339–344, 2012.

[55] S. Chowdhury and K. M. Salahuddin, “A Literature Review of Factors Influencing Implementation of Management Information Systems in Organizations,” vol. 12, no. 8, pp. 72–79, 2017.

[56] E. A. Rigon, C. M. Westphall, and D. R. Dos Santos, “A cyclical evaluation model of information security maturity,” Inf. Manag. Comput. Secur., vol. 22, no. 3, pp. 265–278, 2014.

[57] Saleh, M. F. “Information Security Maturity Model,” International Journal of Computer Science and Security (IJCSS), vol. 5, no. 3, p. 21, 2011.

[58] Y. Goksen, E. Cevik, and H. Avunduk, “A Case Analysis on the Focus on the Maturity Models and Information Technologies,” in Procedia Economics and Finance, pp. 208–216, 2015.

[59] H. Stewart and J. Jürjens, “Information security management and the human aspect in organizations,” Inf. Comput. Secur., vol. 25, no. 5, pp. 494–534, 2017.

[60] M. Zammani, R. Razali, and D. Singh, “Factors contributing to the success of information security management implementation,” International Journal of Advanced Computer Science and Applications, vol. 10, no 11, pp. 384–391, 2019.

[61] ISO, “ISO/IEC 33004:2015 - Information technology — Process assessment — Requirements for process reference, process assessment and maturity models,” 2015.

[62] Stevens, S.S., “On the theory of scales of measurement”, Science, vol. 103, no. 2684, pp. 677-680, 1946.

[63] Sarle, W.S., “Measurement theory: Frequently asked questions,” Disseminations of the International Statistical Applications Institute vol. 1, no. 4, pp. 61-66. 1995.